U.S. Department of Justice

United States Marshals Service

Arlington, Virginia

IOD

U.S. Marshals Service Mobile ID Pilot
Operational Guidelines

(b) (7)(E)

[redacted]

Hit responses will be returned in the following format:

(b) (7)(E)

[redacted]

When capturing a subject's fingerprints with a mobile biometric device this is considered a search. The collection/capture of fingerprints can only be conducted under the following circumstances.

(b) (7)(E)

[redacted]

Prepared by Acting Senior Inspector (b) (6), (b) (7)(C), (b) (7)(E)

April 30th, 2013

Instructions

U.S. Department of Justice
United States Marshals Service

Requisition for Procurement of Supplies, Service, and Equipment

1. REQUISITION NO.:	2. REQUESTED BY (Name/Title/Organization):	TEL NO.:	3. DATE:
	(b) (6), (b) (7)(C), (b) (7)(E) SENIOR INSPECTOR / USMS	202-307(b)	8/25/2014

4. ORGANIZATIONAL BUDGET OFFICER: I do hereby certify that funds are available and authorize an increase of funds but not to exceed $100.00.

NAME _____ TITLE _____

SIGNATURE _____ DATE _____

4a. APPROVAL by Component Head, U.S. Marshal or Designee:

NAME _____ TITLE _____

SIGNATURE _____ DATE _____

5. DELIVER TO:

☒ USMS Warehouse
(b) (6), (b) (7)(C) [redacted]

☐ Requisition forwarded to warehouse on (date): _____

6. SOURCES OF FUNDING:

- ☐ Appropriated
- ☐ Other: _____
- ☐ Reimbursement Auth. No.: _____
- ☐ AFF Case No.: _____
- ☐ District Funds
- ☐ Non-Appropriated

6a. PROGRAM APPROVALS: (Attach before sending to applicable Contracting Office for processing)

- ☐ Financial Services Division: Budget Execution Team (Any Requisition $100K and over) Procurement Chief (Economy Act, Set-Asides, Bureau Proc. Chief as required by FAR/JAR)
- ☐ Information Technology Division: IT (All hardware, software, services, regardless of value) Communications (FAX, Cellular, Pagers, Telephone Equip. & Maintenance
- ☐ Management Support Division: Motor Vehicles (Leases and Repairs) Publishing Services (Copies and Printing)
- ☐ Investigative Operations Division: ESU Equipment
- ☐ Tactical Operations Division: Wireless Communications Equip. (Radios, Repeaters, etc.)
- ☐ Director: Economy Act, J&As, HCA as required by FAR/JAR
- ☐ Deputy Director: Non-Standard Ammo.; Weapons: Service, Backup, Tactical & Defensive; Aircraft Lease or Purchase, New Requirements Over $100K
- ☐ USM, CDUSM or AD: Paid Advertisements
- ☐ OTHER: _____

7. STOCK NO. (a)	ITEM DESCRIPTION (b) Include Accounting Classification Structure (ACS) with each line item. Attach SOWs, Justifications & Other Documentation. Include make, model or salient characteristics.	OBJECT CLASS (c)	UNIT OF ISSUE (d)	QUANTITY (e)	UNIT COST (f)	TOTAL COST (g)
75-0501-1641-9	(b) (7)(E) [redacted]		1	5	(b) (4) [redacted]	$13,950.00
75-0501-3057-6			1	5		$870.00
75-0501-1633-6			1	5		$605.00
Justification:	For use in investigative operations.					

8. ACCOUNTING CLASSIFICATION STRUCTURE:

Fiscal Year *Fund Code* *Organization Code* *Project Code*

9. DC NUMBER:

10. ESTIMATED COST:

TOTAL: **$15,425.00**

(For acquisitions of property, $50,000 or more per item)
APPROVED BY THE OFFICE OF PROPERTY MANAGEMENT:

SIGNATURE _____ DATE _____

VENDOR INFORMATION:

Suggested Source: (b) (7)(E) [redacted]
Contact: (b) (6), (b) [redacted] Phone: 703-286(b) [redacted]
Date Ordered: Date Received:
Order No.:

PRIOR EDITIONS ARE OBSOLETE.
This requisition is not to be used for printing, duplicating, composition graphics or visual production requirements. Use Form USM-219.

United States Department of Justice
Office of Privacy and Civil Liberties (OPCL)

Initial Privacy Assessment (IPA) Instructions & Template

(Revised March 2010)

What is an Initial Privacy Assessment? An Initial Privacy Assessment (IPA) is the first step in a process developed by OPCL to assist DOJ components in the development and use of information systems. Specifically, the IPA is a tool used to facilitate the identification of potential privacy issues; assess whether additional privacy documentation is required; and ultimately, to ensure the Department=s compliance with applicable privacy laws and policies.

The IPA asks a series of basic questions, the responses to which are reviewed by OPCL to identify privacy concerns that may necessitate changes to the system and to determine whether additional privacy analysis and documentation are required, such as a system of records notice (SORN) or collection notice under the Privacy Act, or a Privacy Impact Assessment (PIA) under the E-Government Act. Once OPCL has reviewed a component=s responses and made its determination, a letter reflecting that determination is sent to the component. (The IPA incorporates the matters previously addressed in the Department's Privacy Threshold Analysis document (PTA), and thus replaces the PTA.)

When should an IPA be completed? An IPA should be completed at the beginning of development of an information system, before commencement of any testing or piloting. (This applies regardless of whether the system is electronic or contains only records in paper form.) Additionally, an IPA should be completed any time there is a significant change to the information system to determine whether there are any resulting privacy issues.

The IPA is designed to be a cross-cutting tool to address the requirements of several different privacy laws and policies. These laws and policies have different scopes of coverage, and each has specific terms and definitions to define that coverage. However, because the IPA is not limited to the terms or definitions of just one law or policy, and to ensure the IPA=s utility as a cross-cutting tool, the term **Ainformation system@** as used in the IPA instructions and template refers to: any process of collection, maintenance, use, or dissemination of information, whether performed manually with paper records, or electronically through the use of information technology (IT) products or design.

Who should prepare the IPA? The IPA should be written and reviewed at the component level through the coordinated effort by the component's privacy officials (e.g., Senior Component Official for Privacy (SCOP), Privacy Act Officer, and/or Office of General Counsel), IT security staff, and the program-specific office responsible for the system.

Where should the prepared IPA be sent? A copy of the prepared IPA should be sent to OPCL via email to **privacy@usdoj.gov**. (For classified IPAs, please call 202-514-0208 to coordinate delivery to Suite 940, National Place Bldg., 1331 Pennsylvania Ave., NW., Washington, DC 20530.)

Once OPCL has received the IPA, it will be reviewed for legal and policy concerns, and OPCL will make a determination as to whether any further privacy documentation will be necessary. OPCL will provide written notice, in the form of a determination letter, to the component when the IPA review is completed. The IPA process is considered completed only upon the issuance of OPCL=s determination letter.

How is the IPA related to the Certification and Accreditation (C&A) process? If an IT system requires C&A from the Office of the Chief Information Officer, OPCL=s determination letter must be uploaded into the C&A Web tool as part of the C&A process. Because the determination letter is the artifact that marks the completion of the IPA process, it is the proper artifact to be uploaded (not the IPA itself). For a system that does not require C&A (such as a minor application running on an already certified and accredited IT system, or a paper-based non-IT system), an IPA still should be completed to determine if a PIA, a SORN, or other related privacy documents are required for the system.

Please prepare the IPA per the guidance provided in the questions on the template below.
(These instructions may be detached before submitting the IPA.)

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

Department of Justice
Initial Privacy Assessment (IPA)

DOJ/OPCL (Rev. 03/2010)

NAME OF INFORMATION SYSTEM: Mobile ID

COMPONENT: Mobile ID Server

COMPONENT PRIVACY POINT OF CONTACT (POC) Name: Ed Bordley Office: OGC Phone: 202-307-8571 Bldg./Room Number: CS3 Email: ed.bordley@usdoj.gov	**IPA AUTHOR** (if different from POC) (b) (6), (b) (7)(C), (b) (7)(F) [redacted]
SYSTEM MANAGER/OWNER (b) (6), (b) (7)(C), (b) (7)(F) [redacted]	**SENIOR COMPONENT OFFICIAL FOR PRIVACY** (if applicable, or if different from POC) Name: Ed Bordley Office: OGC Phone: 202.307.8571 Bldg./Room Number: CS3 Email: ed.bordley@usdoj.gov

IPA REVIEW SIGNATURES	
SYSTEM MANAGER/OWNER (b) (6), (b) (7)(C), (b) (7)(F) [redacted] Signature: Date signed: 5/5/2014 (If signed by System Manager=s/Owner's delegate, please identify delegate): Delegate=s Name: Office: Phone: Bldg./Room Number: Email:	**SENIOR COMPONENT OFFICIAL FOR PRIVACY (where applicable) OR COMPONENT PRIVACY POINT OF CONTACT** Signature: _____ Date signed: _____ (If signed by SCOP=s delegate, please identify delegate): SCOP Delegate=s Name: Office: Phone: Bldg./Room Number: Email:

After obtaining all review signatures, please forward the IPA to OPCL and indicate the date forwarded. Unclassified IPAs should be emailed to the OPCL mailbox: privacy@usdoj.gov. (For classified IPAs, please call 202-514-0208 to coordinate delivery to Suite 940, National Place Bldg., 1331 Pennsylvania Ave., NW., Washington, DC 20530.)

DATE FORWARDED TO OPCL: _____

Note: Submission of an IPA to OPCL marks the beginning of the IPA and privacy compliance processes. The IPA process is not complete until OPCL has reviewed the IPA and issued its determination as to the necessity for any further privacy documentation. OPCL will provide written notice, in the form of a determination letter, to the submitting POC when the IPA review is completed. Once the submitting program receives OPCL=s determination letter, the letter should be uploaded to C&A Web to reflect completion of the IPA process. (The IPA itself should <u>not</u> be uploaded as an artifact.)

I. DESCRIPTION OF THE INFORMATION SYSTEM

1. Provide a description of the information system that details: (a) the purpose that the records and/or system are designed to serve; (b) the way the system operates to achieve the purpose(s); (c) the type of information collected, maintained, used, or disseminated by the system; (d) who has access to information in the system; (e) how information in the system is retrieved by the user; (f) how information is transmitted to and from the system; and (g) any interconnections with other systems.

(b) (7)(E)

[redacted]

2. Which of the following describes the type of information in the system:

_X Electronic only. ___ Combination paper/electronic. ___ Paper only.

3. Is there a Certification & Accreditation record within C&A Web?

__X__ Yes. If yes, please indicate the following:

Confidentiality: ___ Low _X__Moderate ___High ___Undefined

Integrity: ___ Low X Moderate ___High ___Undefined

Availability: ___ Low X__Moderate ___High ___Undefined

_____ No. If no, please identify the FISMA-reportable system, the C&A for which, covers this system.

_____ Do not know.

_____ Not applicable B this system is only paper based.

4. Is this a national security system?

_X____ No. _____ Yes. ____ Do not know.

5. Does the system collect, maintain, use, or disseminate any information about individuals?

_____ No. If no, briefly describe the information collected, maintained, or disseminated by the system.

[If you checked no, STOP here after providing the requested description. No further responses are required, and after obtaining all review signatures on page 1, the IPA should be submitted to DOJ OPCL for final review and determination as to whether other privacy-related documentation will be required.]

__X__Yes If yes, briefly describe the types of information about individuals in the system.

(b) (7)(E) [redacted]

6. Please indicate if any of the following characteristics apply to the information in the system about individuals:
(Check all that apply.)

___X__ The information directly identifies specific individuals.

__X___ The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

___X__ The information can be used to distinguish or trace an individual=s identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to the next question.

_____ None of the above. If none of the above, describe why the information does not identify specific individuals, or how it is intended to be used, such that it will not indirectly identify specific individuals? **[If you checked this item, STOP here after providing the requested description. No further responses are required, and after obtaining all review signatures on page 1, the IPA should be submitted to DOJ OPCL for final review and determination as to whether other privacy-related documentation will be required.]**

7. Does the identifiable information in the system pertain only to government employees, contractors, or consultants?

__X___ No. _____ Yes.

8. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system by a personal identifier?

_____ No. If no, skip to question I.11.

__X___ Yes. If yes, proceed to the next question.

9. Is there an existing Privacy Act system of records notice (SORN) that has been published in the Federal Register to cover this system? (Please consult with your component's SCOP, Privacy Act officer, General Counsel, or OPCL if assistance is needed in responding to this question.)

_X___ No.
_____ Yes. If yes, provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system.

10. Does the system collect any information directly from United States citizens or lawfully admitted permanent resident aliens who are the subjects of the information?

_____ No.

_____ Yes. If yes, are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)? (An (e)(3) statement indicates: (I) the authority for collection of the information; (ii) whether submission of the information is mandatory or voluntary; (iii) the principal purpose(s) for which the information will be used; (iv) the applicable routine uses; and (v) the effects on the individual, if any, of not providing the information.)

_X____ Yes. If yes, provide links to, or attach copies of, any such forms or notices. The data collected are fingerprints, pictures.

_____ No.

11. Are Social Security Numbers (SSNs) collected, maintained or disseminated by the system?

__X___ No. If no, skip to question I.13.

_____ Yes. If yes, could the program that this system supports operate without SSNs?

_____ Yes.

_____ No. If no, explain why.

12. Does the system provide any special protection to SSNs (e.g., SSNs are encrypted, only available to certain users, hidden from all users via a look-up table, only in partial form)?

____ No.

_____ Yes. If yes, describe any special protection provided.

13. Is the system operated by a contractor?

_X___ No.

_____ Yes. If yes, and it is determined that the system is covered by the Privacy Act, then the component must ensure that the contract includes language set forth in the Federal Acquisition Regulation, see 48 C.F.R. ' ' 24.104 and 52.224-1 to -2,

applying the Privacy Act=s provisions to the system.

14. Status of system:

_X__ This is a new system in development. **[If you checked this block, STOP here. No further responses are required, and after obtaining all review signatures on page 1, the IPA should be submitted to DOJ OPCL for final review and determination as to whether other privacy-related documentation will be required.]**

_____ This is an existing system. Please continue with Part II.

II. EXISTING SYSTEMS

1. When was the system developed? System is in Pilot phase and has been since March of 2013

2. Has the system undergone any significant changes since April 17, 2003?

   _____ No. If no, skip to question II.5.

   _____ Yes. If yes, explain the nature of those changes. After providing the requested explanation, proceed to the next question.

3. Do the changes to the system involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system?

   _____ No. _____ Yes.

4. Please indicate if any of the following changes to the system have occurred: (Check all that apply.)

   _____ A conversion from paper-based records to an electronic system

   _____ A change from information in a format that is anonymous or nonidentifiable to a format that is identifiable to particular individuals.

   _____ A new use of an IT system, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

   _____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

   _____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

   _____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

_____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system.

5. Does a PIA for this system already exist?

_____ No.

_____ Yes. If yes:

a. Provide the date and title of the PIA and whether the PIA is posted on the web (and if so, include the link):

b. Has the system undergone any significant changes since the PIA?

_____ No. _____ Yes. If yes, describe.

[After obtaining all review signatures on page 1, the IPA should be submitted to DOJ OPCL for final review and determination as to whether other privacy-related documentation will be required.]

U.S. Department of Justice

United States Marshals Service

Washington DC

DC Superior Court

Sole Source Justification

Requisition No.

(b) (5)

[redacted]

September 5, 2013

THIS IS A DRAFT AND IS NOT THE OFFICIAL APPROVED DOCUMENT

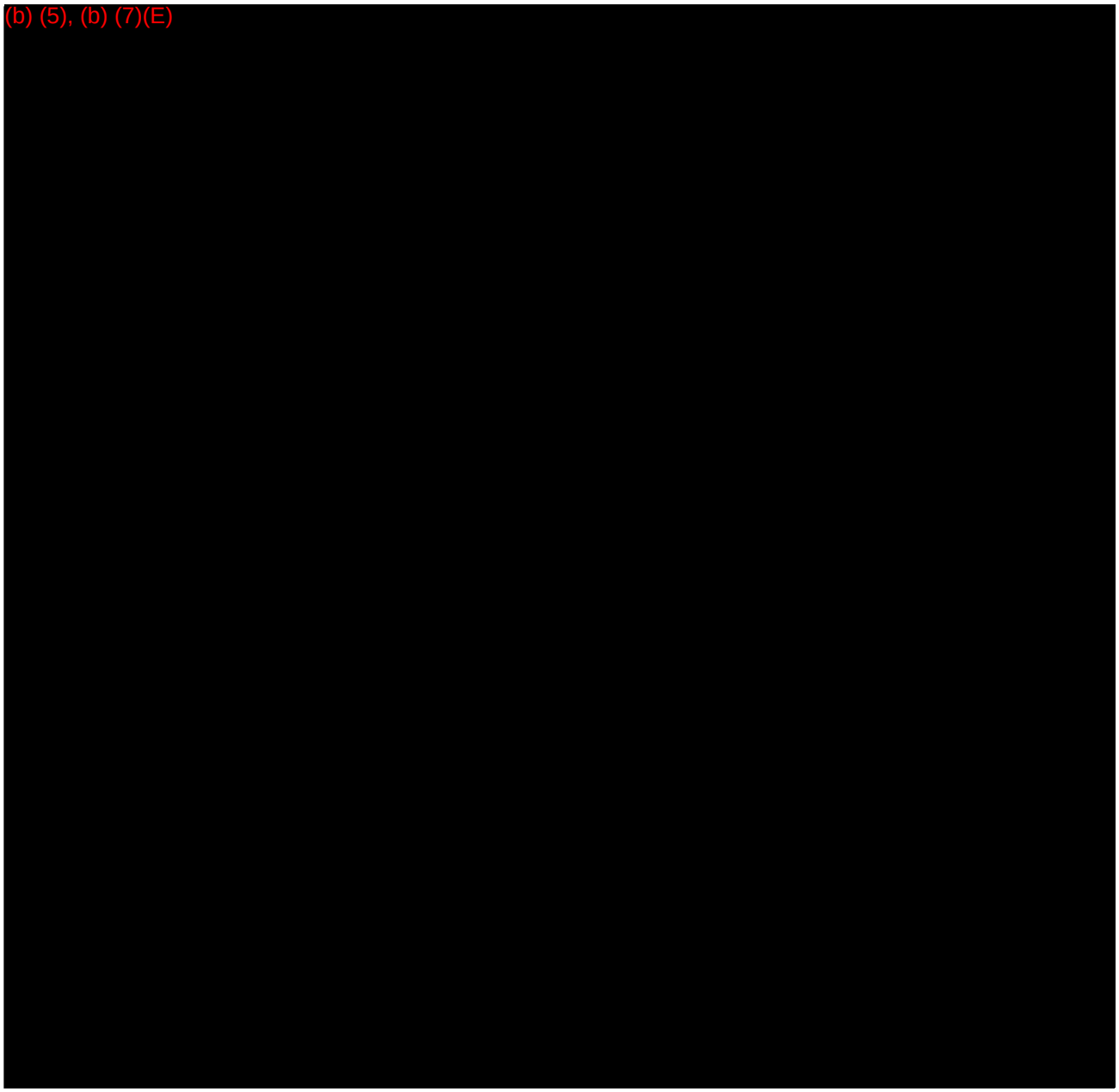
Guidelines for Use of Mobile Identification Devices (Biometric)

(b) (5), (b) (7)(E)

USMS Mobile Biometric Software Requirements

(b) (5), (b) (7)(E)

(b) (5), (b) (7)(E)


(b) (5), (b) (7)(E)

USMS Mobile Biometric Hardware Requirements